IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

INCREASING RATE OF CYBERCRIME CASES IN INDIA AND THE LEGISLATIVE FRAMEWORK

Chhavi Ahlawat[1]

ABSTRACT

Currently, most human activities rely increasingly on Information Technology which is an outcome of fusion of both, communication and computer technology. Because of the development of technology, man now relies entirely on the internet. Internet has enabled the efficient and instantaneous interchange of information throughout the globe, transforming the world into a global village.[2] Internet can be used for various purposes such as social networking, online shopping, online studying, online jobs, and anything else that man can imagine. Access to knowledge is no longer hindered by obstacles of distance and cost, as a result of the information revolution's profound impact on society. Thus, the usage of Information Technology is evident in nearly every aspect of life and has become significant source of growth, trade, communication, entertainment, and adventure.[3] As a result of society's growing reliance on technology, cybercrime has become a significant problem in India. Cybercrime is diverse from other types of crime that take place in society. Reason being, it has no geographical limits and because of less awareness, majority of people still do not know who the cybercriminals are. It has an impact on all parties involved, including the government, industry, and individuals. With rising usage of information and communication technologies in India, cyber-crime is on rise (ICT). Man can become an easy prey to cybercrime as it takes just a single click on internet that all the data and personal information can be retrieved. Lack of awareness among people in India fuels such crime.

Keywords: Information Technology, Internet, global village, cyber-crime, ICT.

INTRODUCTION

Information Technology has acted as a boon for the development of the nation but cybercrime has now become one of the greatest future concerns for law enforcement. As Information and Communications Technology (ICT) becomes progressively more prevalent, electronic crime too becomes a component of all types of criminal

[1] Research Scholar, Department of Law, Central University of Haryana, Mahendragarh, Mob No. 9667217949.
[2] Chernihiv Polytechnic National University and Yuliia Tkach, "CONCEPTUAL MODEL OF CYBER SPACE SECURITY" *Technical Sciences and Technologies* 96-108 (2020).
[3] Yanping Zhang et al., "A survey of cyber crimes: A survey of cyber crimes," 5 *Security and Communication Networks* 422-37 (2012)..

behaviour, including what are today considered "conventional offences." Beginning in 1970s, telephone connections were frequently used by criminals to perpetrate crimes. The criminals were known as Phreakers. In reality, cybercrime didn't really subsist until 1980s. To search/copy/change private data and information, one person had access to another person's computer. Lan Murphy, alias Captain Zap, was first person to be convicted of a cybercrime, in 1981. He broke American Telephone Company's computer system and changed its internal clock to allow consumers to still create free calls in hectic hours.

During period of pandemic, the cybercriminals took advantage of the new normal that was taking over the world in 2021 by attacking remote workers, COVID vaccine research, and a variety of other organizations through opportunistic cyber-attacks in order to disrupt supply chains and networks, further their geopolitical agendas, among other heinous deeds.

Cybercrime plays a role in numerous transnational crimes involving drug trafficking, human smuggling, and money laundering. As most of us are aware, the world has embraced technology enthusiastically and is among the top nations in terms of Internet infrastructure, penetration, and activity. This rapid expansion in the use of computer technology has facilitated a country's participation in the burgeoning Information Economy, but it has also increased the country's vulnerability to electronic crime.[4]

MEANING OF CYBERCRIME AND ITS SCOPE IN INDIA

The word "cyber-crime" typically refers to a broad variety of illegal behaviors that specifically relate to computers and supporting telecommunications infrastructure. Yet, it is widely acknowledged that the term "cybercrime" refers to any illegal conduct carried out with or against digital technology. In other words, they are crimes that occur online or utilize the Internet as a medium. They encompass prohibited actions in ample range. As of internet's inherent anonymity, numbers of worrisome behaviors are taking place in cyberspace, which could permit perpetrators to connect in variety of criminal actions, which are referred to as cybercrimes.

Technology is the tool used in cybercrimes, thus those who perpetrate them are typically technically adept individuals who have a deep understanding of the internet and computer programs. Cyber-stalking, cyber-terrorism, email spoofing, email bombing, cyber-pornography and so on are a few of the most recent cybercrimes to arise. The definition of cybercrime is neither defined in the Act of 2000[5] nor in any other law or statue. Therefore, it is more accurate to define cybercrimes as those crimes in which a computer either serves as the target/ subject/or both. There is little distinction between cybercrime and traditional crime. The involvement of the virtual cyber media, i.e., the computer, at any step is a requirement for cybercrime. Hence, crimes committed against a computer, its system or network, are considered cybercrimes. According to the Act, a voluntary and intentional act/omission that has negative impact on person, their property, or their computer systems, is considered a cybercrime in India.

[4] Atul Jain, *Cyber Crime*: *Issues, Threats and Management* (Isha Books, New Delhi, 2005).
[5] The Information Technology Act, 2000, (Act 21 of 2000).

India is not an exception to the fact that computer-related crime has already grown to be a major source of concern for most nations in the world. The first criterion for determining whether a specific computer-related behavior should be classified as cybercrime is the need to distinguish between what is unethical and what is unlawful. Only when a conduct is actually prohibited should it be treated as crime and the offender must be sought out for prosecution.

CYBERLAWS AND THEIR IMPACT IN DIGITAL WORLD

The term "cyber law" refers to any legal decisions, statutes, and constitutional clauses that have an impact on people and organizations, who manage access to cyberspace, govern who can enter it, develop the technology and software needed to do so, or use their own equipment to access it. If one looks at the aforementioned description, the phrase "access to cyberspace" serves as the fundamental notion of cyber laws. Cyberspace is a new digital medium, and regulations are needed to control how people behave there. These laws collectively are referred to as cyber laws. It is essential to remember that the main goal of cyber laws is to control human conduct, not technology and they heavily rely on technology and encourage technology use but not technological abuse. Cyberspace needs its own law.

The cyber law provisions would apply to any unlawful, improper, or dishonest act carried out online. But, cyber law would expand its scope to bind all people and machines that enter cyberspace. As cyber law is expanding quickly. One must be aware of the three fundamental components of cyber laws, namely:

(a) Netizens (b) Cyberspace and (c) Technology.

I. Netizens

A netizen uses the Internet to extend his physical environment in his daily life by travelling across time and space at click of mouse without recognizing any physical or geographical boundaries but with a limitless potential. The most intriguing aspect of being a netizen is that, he can engage in all kinds of activities while remaining anonymous, nameless, and faceless. It is for these netizens that cyber laws have been created.

II. Cyberspace

Cyber law acts as a bridge between the physical world and the internet. The current cyber rules are an extension of physical laws in cyberspace, it is crucial to remember this. Technically, cyberspace is connected to the physical world by partals, which let people view what is inside. In a nutshell, cyberspace is a conceptual collegium where the world's information resources converge without being visible or audible.

III. Technology

Cyber regulations require a lot of technology. There are two schools of law devoted to technology. Technology Specific School contends single set of technology that should be recognized lawfully, but discourages technical

advancements and aids in developing monopolistic businesses which are detrimental to the community. Technology Neutral School contends that law should remain impartial while recognizing any technology standards and respects all technological advancements or standards equally, but develops various technological platforms, which could raise cost of technology adoption for entire community.

LEGAL FRAMEWORK FOR INDIAN CYBER LAWS

The primary source of cyber law in India is IT Act of 2000, which went into effect on October 17, 2000. Primary objectives of Act are to legalize e-trade and to make it simpler to submit e-records to government. Act also criminalizes many cybercrimes and imposes severe penalties (penalties of up to 10 years in prison and fines of up to Rs 1 crore). The Order with regard to the removal of Information Technology related issues, which was adopted on September 19, 2002, made minor corrections to the Act.[6] Instructions relating to Act provisions regarding protected systems and applications for the issuance of a digital signature certificate were contained in an Executive Order dated September 12th, 2002.

The Act of 2002 which introduced the amendments and miscellaneous provisions with respect to the Negotiable Instruments, made changes to the IT Act.[7] This presented the ideas of shortened checks and computerized checks. The rules with respect to the usage of Electronic Record and Digital Signature in Information Technology, which came in the year 2004, have given the government the legal foundation which it needs to accept papers for filing and to provide licenses.[8] Additionally, it stipulates how fees should be paid to and received by government organizations. The Regulations for the IT outline the qualifications, selection, and duties of Certifying Authorities (CA) and also specify the technological requirements, processes, and security measures that a Certifying Authority must follow. These regulations underwent amendments in the year 2003, 2004 and 2006 respectively.

LEGAL FRAMEWORK OF CYBERLAWS IN INDIA

The Code of 1860[9], was used to prosecute all computer-related crimes because there was no separate and independent cyber law in place prior to the passage of the Act of 2000[10]. Due to the increased reliance on e-commerce as well as e-governance, number of legal-issues relating to computers usage, internet, digital processing devices like IP rights infringement, piracy, jurisdiction, and so on emerged, that couldn't be resolved by current laws which presented practical challenges for law enforcement agencies in policing citizen cyberspace transactions both within and between nations. Although internet-user is technically bound by country's laws wherein they reside, this general rule is challenged when disputes are of a transnational nature. Parliament (of India) passed Information Technology Act to enable electronic filing of documents with government agencies, to legally recognize transactions acted upon via electronic data interchange and other forms of electronic communication, also

[6] Information Technology (Removal of Problems) Order, 2002.
[7] Negotiable Instruments (Amendments and Miscellaneous Provisions) Act of 2002, (Act 55 of 2000).
[8] The Information Technology (Use of Electronic Record and Digital Signatures) Rules, 2004,
[9] The Indian Penal Code, 1860, (Act 45 of 1860).
[10] The Information Technology Act 2000. (Act 21 of 2000).

called "electronic commerce," which involves using alternatives to paper-based methods of communication and information storage. Act's Preamble sought to amend Code of 1860, [11] Act of 1872[12], Act of 1891[13], and Act of 1934[14] in addition to granting legal recognition for e-commerce, facilitating e-filing of documents with government agencies, and providing legal recognition for e-commerce. Act thus establishes legal framework, ensuring all e-records and other actions conducted via electronic means are given legal sanctity.

There have been numerous international conventions and accords to develop a uniform legal strategy for the prevention of borderless cybercrime, these attempts have failed due to a lack of member countries' desired cooperation and initiative. In addition, because different nations' socioeconomic and cultural circumstances determine how sensitive and concerned they are about cybercrimes, countries that are less affected by these crimes are bound to respond differently from those that are severely afflicted. Given the situation, assuming that all nations will tackle the prevention and control of cybercrime in the same way is pointless. Perhaps this is the main reason why different nations haven't actively worked together to establish a global cyber law that would be consistently applied to all of the world's nations. Although a global cyber law has not yet been developed, countries around the world are becoming more and more aware of the need for one as a result of the expansion of the internet, which offers criminals countless opportunities to engage in a range of criminal activities that have transnational or international repercussions.

CYBER-CRIMES: ROLE OF INDIAN JUDICIARY

According to Lord Denning, justice delays are intolerable and a successful judicial delivery system may benefit from information technology.[15] Law in India has advanced significantly since the Information Technology Act, 2000 was passed. Yet, only a small number of cybercrimes have been covered in the offences portion of IT Act, 2000, which was implemented. Significant judicial cases have shown the issues of cyber related crimes which are becoming a major issue especially in the modern world today.

- High Court of Patna ordered for proper inquiry of cyber-crime case wherein charges were put within relevant sections of the Penal Code[16] as well as Act of 2000.[17] It was also noted that local police must be assisted by district level police to investigate cyber-frauds.[18]
- In a landmark judgment, Delhi High Court ruled that "phishing" via internet is unlawful and requires injunction as well as damages recovery.[19]

[11] The Indian Penal Code 1860, (Act 45 of 1860)
[12] The Indian Evidence 1872, (Act 1 of 1872)
[13] The Bankers Books Evidence 1891, (Act 18 of 1891)
[14] The Reserve Bank of India 1934, (Act 2 of 1934)
[15] *Allen* v. *Sir Albert McAlpine and Sons Ltd.*, (1968) 2 Q.B. 229.
[16] The IndianPenal Code, 1860 (Act of 1860) ss. 419, 420
[17] The Information Technology Act 2000 (Act of 2000) s. 66(B).
[18] *Shiv Kumar* v. *the State of Bihar & Ors*., AIR 2021.
[19] *National Association of Software and Service Companies* v. *Ajay Sood & Others*, (2005) DLT 596

- In another case, issue with regard to jurisdiction was raised wherein contract between parties, residing at different places, was made via email.[20]
- Apex Court, in its another decision ruled that in addition to the punitive provisions of IT Act 2000, offences under the IPC, 1860 would also be applied in cases of hacking and data theft.[21]
- In another decision, it was found out through investigation it was found out that mobile phones and computers were used in order to carry out terrorist plan to attack Red Fort. On such facts, appellant was held guilty for offences punishable under the relevant sections of the Penal Code of India. [22]
- In another case, Apex court ruled that in order for a court to have jurisdiction to hear a case, it must also have power to grant requested orders. It must have authority to hear the issue and render a decision on it. The jurisdictional principle must be taken into consideration in order to determine whether the courts' jurisdiction over the internet is exclusive or non-exclusive.[23]

CONCLUSION AND SUGGESTIONS

From foregoing discussion, it can be stated that educating those who are less technologically inclined about risks of cyber related crime and what constitutes criminal action versus noncriminal activity is today's educators' task. Humans are superior to all other living forms on earth and have been endowed with numerous unique faculties, including capacity for thought, analysis, and appropriate action, among others. The pursuit of novel and creative ideas has enabled significant advancement in all aspects of life. From cave age to information age, it has been a long trip for us, and today we rely on technology, particularly information technology, in almost every aspect of our lives. World is currently experiencing information revolution that hasn't ever been experienced before.

With introduction of computers and later computer networking, process of storing and accessing information has been made much simpler. As a result, communication barriers like time and location were eliminated. Technology has advanced to point where things are moving quite quickly for this generation. If we are destined to perish if we do not adapt to the changes occurring around us, there is no time for complacency and we don't get any time to breathe. Next surge in economic growth is being driven by evolving technology. We'll need to employ new technology as well as new ways of thinking to benefit from that expansion. Information technology emerged as most significant technology in final decade of 20th century, revolutionizing people's lives on a worldwide scale to the point where the globe has essentially become a village.

Data is essential to the commission of numerous cybercrimes and the creation of cyber-crime vulnerabilities. Although data offers its users (individuals, businesses, organizations, and governments) countless options, these advantages can (and have) been misused by some for illegal ends. In particular, without the users' informed agreement, choice, and the required legal and security precautions, the huge collection, storage, use, and distribution of data facilitates many cyber-crimes. However, governments and organizations are ill-prepared for the

[20] *P R Transport Agency* v. *Union of India*, AIR 2006
[21] *Jagjeet Singh* v. *State of Punjab*, AIR 2021
[22] *Mohd. Arif @ Asfaq* v. *State of NCT of Delhi*, AIR 2004 SC 1253
[23] *Union of India* v. *Tarachand Gupta*, AIR 1971 SC 1558

scales at which data is gathered, analyzed, and transferred, which raises a host of cyber-security threats. Systems, networks, and data security, as well as privacy and data protection, are interconnected. Due to this, security measures that safeguard data and user privacy are required to combat cyber-crime.